Richmond Hill
Primary Academy

Online Safety Policy

Draft

2017/2018

Policy Monitoring

Development, Monitoring and Review of this Policy

These are the key people involved:

Position	**Name(s)**
School Online Safety Coordinator / Officer	Claire Dutton
Principal	Deborah Secker
Designated Safeguarding Lead	Kelly Cousins
ICT Technical staff	Des Smith
Directors	Mavis Latham

Schedule for Review

This Online Safety policy was approved by the Governing Body:	March 2017
The implementation of this Online Safety policy will be monitored by:	Senior Leadership Team Designated Safeguarding Lead: Kelly Cousins Online Safety Coordinator: Claire Dutton ICT Technical Staff: Des Smith
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the Online Safety policy generated by the monitoring group and Online Safety Coordinator at regular intervals:	Termly
The Online Safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2018
Should serious Online Safety incidents take place, the following external persons / agencies should be informed: *There is a list of agencies that are available to support with / report on concerns of a particular nature (e.g. CSE, inappropriate content) – see 'Support Services' heading at end of policy document*	LA Safeguarding Unit: *01302 737777* Police Liaison Officer: *PC Anette Flavel: 07775031581*

ONLINE SAFETY POLICY March 2017

- The Online Safety Policy relates to other academy policies including those for Safeguarding and Student Protection, Anti-bullying and Computing.
- The academy's Online Safety Coordinator is the Computing Lead, who works under the supervision of the DSL (Designated Safeguarding Lead) and the Senior Leadership Team.
- This Online Safety Policy is informed by DfE guidance, including *Keeping Pupils Safe in Education (2016)*.

Contents

Appendices attached:

1. *Internet and Online Safety Agreement for Staff*

2. *Statement for Academy Employees on the Abuse of the Internet*

3. *Student Acceptable Use Agreement*

4. Termly Review Checklist

Online Safety - DFE Guidance

The use of technology has become a significant component of many safeguarding issues, including: child sexual exploitation; radicalisation; sexualisation; and, sexual predation. Technology can be used as a platform which facilitates harm. An effective approach to online safety empowers a school or college to protect and educate their whole community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material

- Contact: being subjected to harmful online interaction with other users

- Conduct: personal online behaviour that increases the likelihood of, or causes, harm

Filters and monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the academy or colleges IT systems. As part of this process governing bodies and proprietors should ensure their academy has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the schools IT systems and the proportionality of costs verses risk.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part of the risk assessment required by the Prevent Duty.

Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety, including sexting. This will include a clear policy on the use of mobile technology in the school including mobile phones. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Staff Training

As part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding (inc. online concerns) governors and proprietors should ensure that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Governing bodies and proprietors should ensure that all staff members undergo safeguarding and child protection training at induction and that the training should be regularly updated. Induction and training should be in line with advice from LSCB (Local Safeguarding Children Board.

Governing bodies and proprietors should ensure children are taught about safeguarding (inc. online concerns and sexting) through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through personal, social, health and economic education (PSHE) lessons and/or through sex and relationship education (SRE). *At RHPA, children access discreet half-termly Online Safety and Prevent sessions.*

Overview of Response to Risk

Assessing risks

- The academy takes all reasonable precautions to prevent access to inappropriate material. However, due to the scale and nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the academy network. The Academy cannot accept liability for any material accessed, or any consequences of internet access
- The academy will audit ICT provision regularly to establish if the e-safety policy is adequate and that its implementation is effective
- The academy will ensure that monitoring of software and other appropriate procedures are in place to highlight when action needs to be taken by the academy
- The academy will liaise with suitable external agencies and e-Safety consultants where any online safety concerns are raised beyond the knowledge and understanding of the school
- The academy will liaise with partnership academies and other local organisations to establish a common approach to e-safety

System Security

Information system security

- Academy ICT systems, capacity and security are reviewed regularly – making use of external agency expertise where necessary
- Virus protection is updated regularly with reviews considered termly as well as in response to any concerns / issues raised between planned reviews
- The academy's firewall system (updated: March 2017) is in line with current risks and concerns, including prevent legislation. Further updates will be actioned as and when future reviews recommend.

Managing filtering

- The academy will work with their service provider to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover an unsuitable site, it must be reported to the Designated Safeguarding Lead and Online Safety / Computing Lead immediately. The device must be left untouched and taken straight to SLT / Des Smith for action.
- As part of their termly review, the Online Safety / Computing Lead will ensure that checks are made to ensure that the filtering methods selected are appropriate – whilst also responding appropriately to any concerns raised between planned reviews

Personal Data and Contact Details

Protecting personal data

- Personal data are recorded, processed, transferred and made available according to the Data Protection Act 1998

Published Content via Academy Website and Twitter

- The contact details on the website are the academy address, e-mail, telephone number and sometimes photos. Staff or pupils' personal information will not be published
- The Principal takes overall editorial responsibility and ensures that content is accurate and appropriate

Pupils' images and work

- Photographs that include pupils are selected carefully and will not enable individual pupils to be clearly identified without parental consent
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers for the use of photographs on the website is requested as part of the annual data collection process – such permissions are advised to staff at the start of the academic year and made readily available as required

Technology in School

Managing emerging technologies

- Emerging technologies are examined for educational benefit and risk assessments are carried out before use in academy is allowed – at which point, updates to policy and home/school agreements should be made
- The academy recognises that technologies such as mobile phones with wireless internet access and 'wearable technology' such as smart watches can bypass academy filtering systems and present a new route to undesirable material and communications – steps taken to limit the risks involved are included in this policy

Visitors and their technology

- Visitors to school are not permitted to use their personal devices within the academy site unless given permission by the principal

- Visitors are not permitted to photograph, video or use technology with pupils unless express permission is granted by the principal and this must only be done via an academy device – not on the visitor's personal device
- The academy can accept no responsibility for loss or damage to technologies brought onto school premises by visitors

Complaints / Non-Compliance

Handling online safety complaints

- Any concerns or notification of incidents involving online safety must be reported immediately to the Designated Safeguarding Lead for consideration / further referral and possible action as well as being recorded on CPOMs
- Any complaint about staff misuse must be referred to the Principal and if the alleged misuse is by the Principal it must be referred to the Designated Safeguarding Lead and the academy's directors and/or Governors
- Any staff misuse that suggests a crime has been committed, a pupil has been harmed or that a member of staff is unsuitable to work with pupils must be reported by the Principal to the Designated Safeguarding Lead and academy's Governors
- Pupils, parents and staff are informed of the complaints procedure

Staff and the e-safety policy

Staff awareness

- All staff are made aware of the academy's online safety policy and its importance explained via the 'Statement for Academy Employees on the Abuse of the Internet' (Appendix 2)
- All staff, including those not directly employed by the academy, who require access to the academy's internet system are required to sign the 'Internet and Online Safety Agreement' (Appendix 1)
- A copy of the policy is available to staff via the academy's staff server, as well as the website
- All staff have a responsibility to ensure this policy is adhered to by both themselves and others, and a duty to report any breaches or concerns about conduct relating to this policy
- Staff are made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential at all times

- Staff must adhere to the academy's *Staff Code of Conduct* - if a member of staff breaches the restrictions put forward by this policy then disciplinary action may be taken

Staff emails

- Staff should not use personal email accounts to communicate with service users
- Staff should not use work email accounts for personal purposes

Staff use of work devices

- Staff should only use work devices (e.g. laptop, iPad, etc.) for their designated purpose
- Staff in charge of school devices are responsible for their care and security. All reasonable measures should be taken to ensure the correct care of the device and to ensure it is kept secure both on- and off-site.
- Where staff make recordings (i.e. image, audio, video, etc.) of pupils using school devices, they are responsible for deleting those recordings once they have been assessed or transferred to the relevant medium
- All school devices which hold school related data and recordings must be password protected / stored securely within the school premises
- Staff are responsible for keeping their work-related passwords and accounts safe and secure. Passwords should not be shared. Devices should be secured when left unattended (e.g. laptop should be set to 'sleep' when staff member leaves their desk / room – however briefly)
- Staff should not save any work-related information or recordings of pupils in an unsecure fashion (e.g. unencrypted memory stick). Staff should save any work-related documents, data or recordings via the online Outlook 365 portal or, as a temporary measure only, on a secure school device (e.g. desktop on laptop, iPad)
- Staff should not use work devices to access personal accounts which are not work related (e.g. social networking sites)
- In line with the Academy's *Staff Code of Conduct*, staff should not download or stream from sources whose security is questionable in any way or for uses which are not school related. If in any doubt about security of a website, staff should refer to the ICT Technician before attempting download
- Staff are responsible for ensuring they act in accordance with copyright laws when copying or downloading for work or other purposes

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting pupils within or outside of the setting in a professional capacity

- Mobile phones and personally-owned devices are switched off or switched to 'silent' mode at the academy, unless permission has been granted by the principal. Such devices should be stored securely out of sight and never used in the presence of pupils (except in an emergency or where permission has been granted by the Principal)
- Bluetooth communication should be 'hidden' or switched off
- Staff must not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose
- In an emergency where a staff member doesn't have access to an academy-owned device, they should use their own device and hide their own mobile number for confidentiality purposes (e.g. an emergency during a school visit away from the academy site)
- Staff should not allow pupils to wear / use the staff member's personal device at any time

Wearable Technology

- Wearable technologies, such as smart watches, are permitted in so long as they do not interfere with staff's responsibilities
- Wearable technology should not be used to record images, audio or video within the academy
- Staff are responsible for making their own risk assessment with regards to wearable technologies and are subsequently responsible for loss or damage which may occur as a result of use in school.

Social networking

- Staff are made aware that their use of social networking applications has implications for our duty to safeguard pupils
- Pupils and their parents should not be accepted as friends by staff – any exceptions to this should be reported to the Principal
- All staff should bear in mind that any information or images they share through social networking applications, even if they are on private spaces, are still subject to relevant legislation, including: copyright, data protection, Freedom of Information, safeguarding and others
- Staff must not issue any advice or information in the name of the academy via their personal networking accounts

- Concerns about staff conduct on social networking sites should be directed to the academy principal. Where concerns are about the principal's conduct then the matter should be raised with the Governors

Pupils and the e-Safety Policy

Introducing the online safety policy to pupils

- Online safety rules, in a format appropriate for our pupils, are posted in classrooms and discussed with pupils as part of their learning, wherever appropriate
- Pupils are made aware of the Online Safety Policy through the 'Acceptable Use for Students Agreement' (appendix 3) which they are required to sign in an age-appropriate format
- Pupils are informed that network and Internet use is monitored
- Online Safety and Prevent is given a high priority at the academy and, as such, is taught as a discreet subject in its own right in addition to being embedded throughout other curriculums and experiences
- Online safety training is embedded within the Computing teaching and learning documents as well as the school's SMSC curriculum

Teaching and learning

The internet is an essential element in 21st century life for education, business and social interaction. The academy recognises it has a duty to provide pupils with quality internet access as part of their learning experience, regardless of their learning disabilities and attainment levels. It is also part of the statutory computing curriculum and a necessary tool for staff and pupils. Richmond Hill Primary Academy ensures that:

- All pupils are included in this entitlement
- The academy internet access is designed expressly for student use and includes filtering appropriate to the needs of our pupils
- Teachers are required to consider risks and raise key learning points with pupils regarding online safety and internet use wherever they arise

The academy has developed its own scheme of work (e-Safety and Prevent) which involves pupils in discreet half-termly e-Safety and Prevent learning activities. As part of this approach:

- Pupils receive access to a developmental e-Safety and Prevent curriculum throughout their time in school

- Pupils are taught what internet use is acceptable and what is not, and given clear objectives for internet use, this includes mobile technologies such as i-pads/mobile phones (where sexting is also discussed in an age-appropriate approach)
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils are educated in the effective use of the internet
- Pupils are advised of appropriate online conduct and are made aware of issues relating to negative online conduct, for instance: online bullying, 'banter', racism, incitement, etc.
- Pupils are taught how to critically evaluate internet content and how to adhere to relevant legislation (e.g. copyright)
- Pupils are taught how to respond to inappropriate content, including issues around Prevent
- Pupils are taught how to report inappropriate internet content, contact or conduct - to academy staff; to safe adults or parents; to peers; and, to relevant external agencies (inc. the CEOP button and ChildLine telephone numbers)

E-mail

- Pupils are not given their own e-mail accounts on the academy system, but where appropriate an approved email address for their use is set up for curriculum purposes that is monitored at all times by the class staff
- In an email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- E-mail sent to an external organisation should be written carefully and authorised by SLT before sending, in the same way as a letter written on academy headed paper
- The forwarding of chain letters is not permitted

Social networking and personal publishing

- The academy will block/filter access to social networking sites for pupils
- Pupils are advised of the potential dangers associated with the use of social network spaces outside the academy
- The academy cannot be held responsible for pupils' online behaviours outside of school

Personal Devices

- Pupils are not permitted to use / have on their person any form of personal technology which may pose a risk to themselves, their peers, staff or the academy

(for instance, mobile phones and iPads). Where children do bring such devices to school, they must be stored securely by staff until the end of the day. *Currently, KS2 pupils are permitted (following parental signature) to bring personal devices to school as a security aid when walking to/from school alone. These must be handed into the academy office upon arrival at school and then collected at the end of the day.*

- Where children are using wearable technologies (e.g. smart watches) the class teacher must assess the risk of such a device. Children are not permitted to record, view, stream or share audio, images or video on such devices and if this is a risk then the device must be removed by the child and stored securely by staff until the end of the day
- If members of staff have an educational reason to allow pupils to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the Senior Leadership Team
- The academy can accept no responsibility for loss or damage to technologies brought onto school premises by pupils or their parents/carers.

Home / School and Wider Community Links

Enlisting parents' support

- Parents' attention is drawn to the online safety policy in newsletters, the Academy Offer and through information on the academy Website.
- Parents are supported by information on the safe use of the internet for their families where applicable – inc. leaflets sent home, parent meetings, etc.

Parents in school

- When on school premises parents are subject to the same restrictions as 'visitors' to school
- Where parents are representing school in a 'staff' role (e.g. class helpers, school trip chaperones) they are subject to the same restrictions as staff
- Parents may be permitted to take photographs of their own children on the school premises (e.g. following a school production) but this is at the discretion of the principal / SLT. Where permission is granted, parents must not post images of children - other than their own - on any social networking sites

Social Media

- Parents are advised to raise any concerns directly with school and never via social media outlets

- The academy cannot be held responsible for any information published outside of its own communication accounts (e.g. school website, twitter account, school app)
- Where the academy feels it is threatened or its staff are subjected to any form of abuse online then reasonable steps to resolve the matter will be taken by the Principal. This may involve taking legal advice / action if necessary

Links with other policies / agendas

Prevent Duty – refer to Prevent Duty Policy

- The academy is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society
- We protect children from the risk of radicalisation, for example by using filters on the internet to make sure they can't access extremist and terrorist material, or by vetting visitors who come into the academy to work with pupils
- The academy's firewall system (updated: March 2017) is in line with current prevent legislation and, as such, its filters limit risk in this area. Further updates will be actioned as and when future reviews recommend.
- Our Safeguarding Children & Young People, Prevent Duty and Online Safety policies sets out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support

Child Sexual Exploitation – refer to Safeguarding Children & Young People policy

- CSE is an important aspect of keeping children safe and the links between CSE and technology are explored by both staff (as part of regular safeguarding training) and pupils (in an age-appropriate way as part of the e-safety/prevent scheme of work).
- Wherever staff have any level of concern with regards to CSE, they should refer to the reporting procedures detailed in the school's safeguarding policy.
- Pupils are, as a minimum, reminded of support/help routes for any concerns (inc. CSE) during each half-termly e-safety/prevent lesson and by displays throughout school. Additional reminders may be highlighted in assemblies or as part of classroom discussions as appropriate.

- Parents have access to information and helplines/links regarding e-safety & safeguarding matters (inc. CSE) via the school website, as well as other forms of communication from time to time (e.g. leaflets sent home; parent workshops).

Video Enhanced Observation (VEO) – *refer to VEO policy*

- The VEO system is used in school for the purposes of professional development for staff. Emphasis is on use of VEO for positive, collaborative development
- At all times, the VEO system should be focused entirely upon teaching and learning aspects within a lesson and not used as a way of recording or monitoring individual children outside of this remit
- Pupils and parents were advised about the VEO system during its launch in March 2017. Permissions were granted in line with the annual home-school agreement, unless permission was expressly revoked by parents following initial advice. Going forwards, VEO will be included in the annual Photographs / Video agreement contract signed by parents
- Staff using the VEO system will be responsible for ensuring permission is available for all children in their recording
- When using the VEO system, staff are responsible for ensuring the video space is correctly signposted so that anybody entering is aware of the recording taking place
- Staff using the VEO system are responsible for uploading their video to the cloud storage system and/or deleting videos from the recording device

Support Services

Additional advice / support and reporting procedures can be found at:

- ***Internet Watch Foundation***

  In the event that a site has no reporting function and if the content is a sexual image of someone under 18 you can report it to the Internet Watch Foundation (IWF). Sexual images of anyone under 18 are illegal and the IWF can work to get them removed from sites which do not have reporting procedures. Adults can report directly to the IWF here – www.iwf.org.uk. Young people can contact ChildLine who work in partnership with the IWF and will support young people through the process.
- ***NCA-CEOP***

If you are concerned that a child is being sexually abused, exploited or groomed online you should report to NCA-CEOP www.ceop.police.uk/safety-centre

- ***NSPCC***

  adults helpline: 0808 800 5002

  The NSPCC has partnered with O2 to offer direct support to parents and other adults on issues relating to online safety.

- ***ChildLine***

  www.childline.org.uk

  ChildLine offers direct support to children and young people including issues relating to the sharing of sexual imagery.

- ***Professionals Online Safety Helpline (POSH):***

  http://www.saferinternet.org.uk/about/helpline Tel: 0844 381 4772

  The POSH helpline supports professionals with an online safety concern or an online safety concern for children in their care. Professionals are able to contact the helpline to resolve issues.

- ***NWG Network Group***

  information and support on child sexual exploitation. The group promotes a National CSE awareness day

  www.stop-cse.org Tel: 01332 585371

Appendix 1: Internet and Online Safety Agreement for Staff

The academy's Online Safety Policy, along with this agreement, has been drawn up to protect all parties (pupils, parents/carers, fellow staff and the academy itself). All staff, including those not directly employed by the academy, requesting ICT/internet access should sign a copy of this Agreement to acknowledge understanding and agreement before returning to the academy.

- All users are responsible for ensuring they are fully au fait with the contents of the Online Safety Policy and subsequently, act in accordance with its advice and restrictions – including any updates to the policy and related policies as they are presented
- All members of staff are responsible for explaining internet safety rules and their implementations to pupils
- All users need to be aware of possible misuses of online access and their responsibilities towards pupils, staff and the academy
- All staff have a duty to report any breaches or concerns about conduct relating to internet use and online safety via the appropriate channel
- Staff are not permitted to use their own devices for contacting or recording pupils at any time. Where there is any reason to deviate from this restriction, even when outside of professional responsibility, then it is the responsibility of the staff member to advise the Principal for the reason of this
- The computer system and any other school technologies are owned by the academy, and may be used by pupils to further their education and by staff to enhance their professional activities including teaching, research, administration and management.
- The academy reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited and email sent or received
- All ICT and Internet activity must only be appropriate to the user's professional activity or the pupil's education
- Access to the school's ICT systems and internet should only be made via the staff member's authorised accounts and passwords, which should not be made available to any other person
- Staff should make all reasonable attempts to take care of their school-owned technology and to keep access to their devices and accounts secure
- Users are responsible for all email sent, including attachments, and for contacts made via their personal work accounts. Any breach may result in email being reserved
- As email can be forwarded or inadvertently sent to the wrong person professional levels of language and content should be applied at all times
- Any activity which threatens (or potentially threatens) the integrity of the academy's ICT systems or that attacks or corrupts other systems, is forbidden – where there is any level of doubt staff should always refer to the academy's ICT Technician
- Use for personal financial gain, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden and is deemed illegal
- Use of mobile devices/phones to create, send or receive sexually explicit photographs is forbidden

Any violation of the above code of conduct may result in a temporary or permanent ban on Internet use. Additional disciplinary action (up to and including dismissal) may be taken in line with existing practice on inappropriate language or behaviour. Where appropriate, misconduct will be reported to the relevant authorities and external agencies.

Appendix 2 Statement for Academy Employees on Abuse of the Internet

The purpose of this policy is to inform staff that abuse of the Internet within the academy is treated extremely seriously with disciplinary action being taken which could lead to dismissal. This statement should be read together with the academy's Online Safety Policy, Internet and Online Safety Agreement for Staff, and any other relevant documents or policies referenced within.

- Where staff are allowed to use the Internet, it is on the clear understanding that abuse will not occur
- All Internet connections and access through the Service Provider's ICT Network are logged and monitored

'Abuse' includes:

- Accessing, displaying, downloading or disseminating pornographic or other 'adult' materials
- Posting information that may tend to disparage or harass others on the basis of gender, race, age, disability, religion, sexual orientation, political affiliation or national origin
- Uploading photographs of Pupils to the Internet
- Publishing statements that are defamatory and could bring the academy into disrepute
- Publishing information that is false or misleading concerning the academy or any other company, organisation or individual that could bring the academy or Local Authority into disrepute
- Any activity that breaches the Data Protection Act including publishing confidential or proprietary information of the academy or Local Authority, or any of its customers or other business associates, on unsecured Internet sites such as Bulletin Boards or disseminating such information that might compromise its confidentiality
- Unauthorised publishing of information not related to the academy
- Knowingly downloading, using, or distributing software or programmes from the Internet without verifying their operational integrity, e.g. checking for the absence of computer viruses and breaching of copyright
- Participating in any form of gambling and personal use of the Internet facilities without the specific consent of the Principal of the academy
- The use of personal social networking sites through academy devices. Further, the use of such sites outside of the academy for the purposes of discussing academy activities / pupils / parents / colleagues

Online Safety and Social Media Guidance for Staff *(in addition to detail in policy)*

Appropriate:

- Set your privacy settings for any social networking site to the highest security available
- Ensure any technological equipment, (including your mobile phone) is password/ PIN protected
- Use professional online accounts/ identities/conduct if you wish to have online contact with service users, their families and other professionals
- Make sure that all publicly available information about you is accurate and appropriate

- Remember online conversations may be referred to as 'chat' but they are written documents and should always be treated as such
- Make sure that you know the consequences of misusing digital equipment
- If you are unsure who can view online material, assume it is public. Remember - once information is online you have relinquished control
- When you receive any new equipment (personal or private) make sure that you know what features it has as standard and take appropriate action to disable/ protect

Inappropriate

- Giving your personal information to service users -pupils/ young people, their parents/ carers. This includes mobile phone numbers, social networking accounts, personal website/ blog URLs, online image storage sites, passwords etc.
- Using your personal mobile phone to communicate with service users. This includes phone calls, texts, emails, social networking sites, etc.
- Using the internet or web-based communication to send personal messages to pupils/young people
- Sharing your personal details with service users on a social network site
- Adding/allowing a service user to join your contacts/friends list on personal social networking profiles
- Using your own digital camera/ video for work. This includes integral cameras on mobile phones
- Playing online games with service users

Appendix 3:
Student Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the academy's computers for academy work and homework
- I understand that network and Internet use is monitored
- I will not attempt to visit Internet sites or conduct online searches that I know to be banned by the academy
- I will only edit or delete my own files and not look at, or change, other people's files without their permission
- I will keep my logins and passwords secret
- I will not bring files into the academy without permission or upload inappropriate material to my workspace
- I understand that any personal technological devices which I bring to school are (a) my own responsibility (b) required to be held securely by the academy until the end of the day (c) not allowed to be used for recording within school in any way
- I am aware that some websites and social networks have age restrictions and that I should respect this
- I understand that there are consequences for negative online behaviours – whether conducted inside or outside of school
- I will not use mobile phones to send inappropriate communication, photographs or videos
- I will only e-mail people I know, or who a responsible adult has approved
- The messages I send, or the information I upload, will always be polite and respectful
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me
- If I see anything I am unhappy with, either for myself or my peers, or if I receive a message that I do not like, I will not respond to it but I will report to a teacher / responsible adult

I have read and understand these rules and agree to them.

Signed:

Date:

Termly Online Safety Checklist

Note: Please send copy to SLT and governing body

Term:

Aspect of Online Safety	**Notes / Action** *(signature & date of reviewer/s)*
Have there been any breaches to the policy?	
Other concerns / incidents to note (inc. external matters raised through wider media)	
Changes to wider policies and practice (e.g. safeguarding, prevent)	
Emerging Technologies / risks to note	
General Technical Review – software; devices; etc.	
Virus Protection Review	
Firewall Protection Review	
Any other matters to note	
Suggested Updates to Policy / Agreements / Practice	